PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04N 7/16, 7/167

A1

(11) International Publication Number: **WO 97/38530**

(43) International Publication Date: 16 October 1997 (16.10.97)

(21) International Application Number: PCT/EP97/01557

(22) International Filing Date: 21 March 1997 (21.03.97)

(30) Priority Data:
96200907.2 3 April 1996 (03.04.96) EP
(34) Countries for which the regional or international application was filed: AT et al.

(71) Applicant *(for all designated States except US)*: DIGCO B.V. [NL/NL]; Jupiterstraat 42, NL-2132 HD Hoofddorp (NL).

(72) Inventors; and

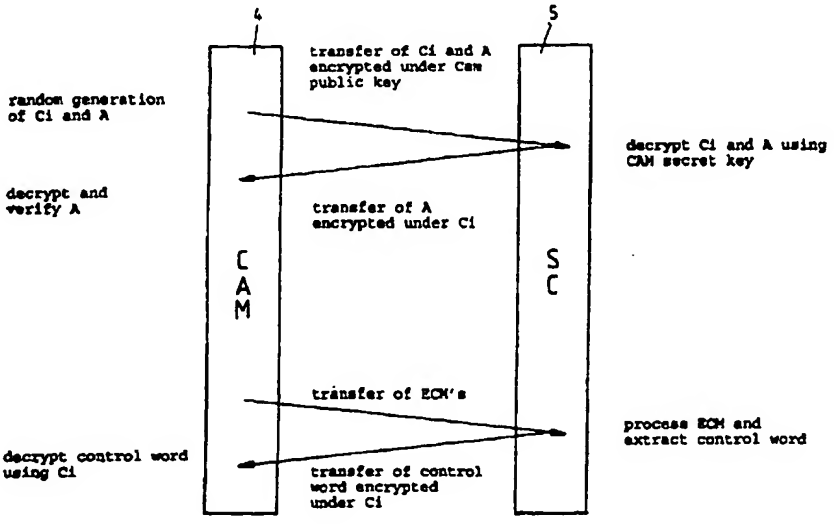
(75) Inventors/Applicants *(for US only)*: RIX, Simon, Paul, Ashley [ZA/ZA]; 51 Ixia Road, Primrose Hill, Germiston, Transvaal (ZA). GLASSPOOL, Andrew [GB/GB]; Telford Point, Telford Road, Basingstoke RG21 2XZ (GB). DAVIES, Donald, Watts [GB/GB]; 15 Hawkewood Road, Sunbury-on-Thames, Middlesex TW16 6HL (GB).

(74) Agents: DE VRIES, Johannes, Hendrik, Fokke et al.; De Vries & Metman B.V., Overschiestraat 184 N, NL-1062 XK Amsterdam (NL).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ARIPO patent (GH, KE, LS, MW, SD, SZ, UG), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: METHOD FOR PROVIDING A SECURE COMMUNICATION BETWEEN TWO DEVICES AND APPLICATION OF THIS METHOD



(57) Abstract

In a method for providing a secure communication between two devices, a first device generates a random key (Ci) and transfers this key to a second device in a first message encrypted using a plublic key. The second device decrypts the first encrypted message by means of a corresponding secret key to obtain the random key (Ci) and this random key is used to encrypt and decrypt all transmissions between these devices. In a decoder for a pay TV system, comprising a conditional access module and a smart card, this method is applied to provide a secure communication between the control access module and the smart card and/or between the decoder and the conditional access module.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

Method for providing a secure communication between two devices and application of this method

The present invention relates to a method for providing a secure communication between two devices, in particular between devices used in a pay TV system.

In a pay TV system each subscriber generally has a decoder for descrambling the source component signal, wherein said decoder comprises a conditional access module and a smart card for decrypting entitlement control messages and entitlement management messages. In order to prevent unauthorized operation of the decoder for descrambling a source component signal it is important to prevent switching between an authorized and an unauthorized smart card for example.

The invention aims to provide a method of the above-mentioned type wherein the communication between two devices, such as the control access module and the smart card or the decoder and the conditional access module, is arranged in such a manner that switching between authorized and unauthorized devices is not possible.

According to the invention a method is provided, wherein a first device generates a random key (Ci) and transfers said key to a second device in a first message encrypted using a public key, wherein said second device decrypts the first encrypted message by means of a corresponding secret key to obtain said random key (Ci), wherein said random key is used to encrypt and decrypt further transmissions between said devices.

According to the invention this method can be applied in a decoder for a pay TV system, wherein said decoder comprises a conditional access module and a smart card, wherein said method is applied to provide a secure communi-cation between the control access module and the smart

card or between the decoder and the conditional access module.

The invention further provides a decoder for a pay TV system, comprising a conditional access module and a smart card, said conditional access module comprising means for generating a random key (Ci), means for encrypting said key in a first encrypted message using a public key encryption method, means for transfering said first encrypted message to the smart card, said smart card comprising means for receiving and decrypting said first encrypted message to obtain said random key, means for encrypting transmissions to the conditional access module under said random key, said conditional access module having means to decrypt said transmissions received from the smart card.

In a further embodiment of the invention, said decoder comprises a conditional access module and a smart card, wherein said decoder comprises means for generating a random key (Ci), means for encrypting said key in a first encrypted message using a public key encryption method, means for transfering said first encrypted message to the conditional access module, said conditional access module comprising means for receiving and decrypting said first encrypted message to obtain said random key, means for encrypting transmissions to the decoder under said random key, said decoder having means to decrypt said transmissions received from the conditional access module.

The invention will be further explained by reference to the drawings in which an embodiment of the method of the invention is explained as applied in a decoder for a pay TV system.

Fig. 1 shows a block diagram of an embodiment of the decoder according to the present invention.

Fig. 2 shows a sequence of steps of an embodiment of the method of the invention.

Referring to fig. 1 there is shown in a very schematical manner a block diagram of a decoder for a pay TV system, wherein digital information signals are scrambled using a control word in accordance with the Eurocrypt

standard for example. In this embodiment the decoder comprises a demodulator 1, a demultiplexer 2 and a decompression unit 3. The decoder further comprises a conditional access module or CAM 4 and a smart card 5 which can be inserted into a connection slot of the conditional access module 4. Further the decoder is provided with a microprocessor 6 for configuration and control purposes.

The conditional access module 4 is provided with a descrambler unit 7 and a microprocessor 8 having a memory 9. The smart card 5 comprises a microprocessor 10 having a memory 11.

As the operation of the above-mentioned parts of the decoder is not a part of the present invention, this operation will not be described in detail. Typically, the signal received by the demodulator 1 is a modulated data stream between 950 MHz and 2050 MHz. The output of the demodulator 1 is a scrambled digital data stream which is provided to the CAM 4 and the descrambler 7 will be allowed to descramble this scrambled data stream assuming that an authorized smart card has been inserted and the subscriber is entitled to receive the program. The descrambled data stream is demultiplexed by the demultiplexer 2 and decompressed and converted into the original analogue audio and video signal by the decompression unit 3.

In a pay TV system the control word required for descrambling, is transferred to the subscribers in so-called entitlement control messages containing the control word encrypted using a service key. This service key is downloaded in the memory 11 of the smart card 5 by means of a so-called entitlement management message for example. During operation the CAM 4 transfers the entitlement control messages towards the microprocessor 10 of the smart card 5 so that the microprocessor 10 can process the entitlement control message and extract the control word. Thereafter the smart card 5 returns the decrypted control word towards the CAM 4 so that the descrambler 7 is allowed to descramble the digital data stream received from the demodulator 1.

In order to prevent the use of an unauthorized smart card 5 in combination with the CAM 4 it is important to provide a secure communication between the CAM 4 and the smart card 5. According to the present invention the following method is used to provide such a secure communication. The steps of this method are shown in fig. 2. When a smart card is inserted into the decoder, the microprocessor 8 of the CAM 4 will generate two random numbers Ci and A. The microprocessor 8 will encrypt in a first message the random numbers Ci and A under a public key of the CAM 4. The thus obtained first message is transferred to the smart card 5 and the microprocessor 10 will decrypt this first message using the secret key of the CAM 4. Thereafter the microprocessor 10 will return a second message to the CAM 4, said second message being the random number A encrypted under the number Ci used as encryption key. The microprocessor 8 of the CAM 4 decrypts this second message and verifies whether the random number A is correct. Assuming that the random number A is indeed correct, so that it may be assumed that the inserted smart card 5 is an authorized smart card, the CAM 4 will then forward entitlement control messages containing the encrypted control word to the smart card 5 which will process the entitlement control message and extract the control word in a conventional manner. However, in the return message towards the CAM 4, the smart card will forward the extracted control word encrypted under the key Ci and these encrypted control words are decrypted by the microprocessor 8 using the same key Ci. As soon as one tries to replace the inserted smart card 5 by an other smart card, for example by switching from the authorized smart card 5 to an unauthorized smart card, the CAM 4 will immediately establish such change as the key Ci will not be known to the new smart card, so that the CAM will no longer be able to descramble the return messages containing the control word. Thereby the descrambler unit 7 will be disabled.

The method described can be used in the same manner for providing a secure communication between the CAM 4 and

the decoder, wherein the same protocol as shown in fig. 2 is followed.

In summary it will be understood that if a new CAM 4 is connected to the other decoder parts, the microprocessor 6 of the decoder will generate the two random numbers Ci and A and as soon as the microprocessor 6 has decrypted the second message received from the microprocessor 8 of the CAM 4, and has verified that the random number A is correct, the key Ci will be used in all transmissions between the CAM 4 and the microprocessor 6.

The invention is not restricted to the above-described embodiments which can be varied in a number of ways within the scope of the claims. As an example for a further embodiment the CAM (i.e. the descrambler) may be part of the decoder. The decoder would now challenge the smart card to authenticate itself to obtain a secure communication between the smart card and the decoder.

CLAIMS

1. Method for providing a secure communication between two devices, wherein a first device generates a random key (Ci) and transfers said key to a second device in a first message encrypted using a public key, wherein said second device decrypts the first encrypted message by means of a corresponding secret key to obtain said random key (Ci), wherein said random key is used to encrypt and decrypt transmissions between said devices.

2. Method according to claim 1, wherein after decrypting said encrypted message, said second device first returns said random key (Ci) in a second encrypted message with an authentication to said first device.

3. Method according to claim 2, wherein for providing said authentication said first device further generates a random number (A) and transfers this random number (A) together with said random key (Ci) in said first encrypted message to the second device, wherein the second device uses said random number (A) for authentication in the second encrypted message.

4. Method according to claim 3, wherein said second device encrypts said random number (A) under said random key (Ci) to obtain said second encrypted message.

5. Application of the method of anyone of the preceding claims in a decoder for a pay TV system, wherein said decoder comprises a conditional access module (CAM) and a smart card (SC), wherein said method is applied to provide a secure communication between the control access module and the smart card.

6. Application of the method of anyone of claims 1-4 in a decoder for a pay TV system, wherein said decoder comprises a conditional access module (CAM) and a smart card (SC), wherein said method is applied to provide a secure communication between the decoder and the conditional access module.

7. Decoder for a pay TV system, comprising a conditional access module and a smart card, said conditional access module comprising means for generating a random key (Ci), means for encrypting said key in a first encrypted message using a public key encryption method, means for transfering said first encrypted message to the smart card, said smart card comprising means for receiving and decrypting said first encrypted message to obtain said random key, means for encrypting transmissions to the conditional access module under said random key, said conditional access module having means to decrypt said transmissions received from the smart card.

8. Decoder according to claim 7, wherein said smart card comprises means for returning said random key to the conditional access module in a second encrypted message with an authentication.

9. Decoder according to claim 8, wherein said generating means of the conditional access module further generates a random number which is included in said first encrypted message, wherein the smart card is adapted to use said random number as authentication in the second encrypted message.

10. Decoder for a pay TV system, comprising a conditional access module and a smart card, wherein said decoder comprises means for generating a random key (Ci), means for encrypting said key in a first encrypted message using a public key encryption method, means for transfering said first encrypted message to the conditional access module, said conditional access module comprising means for receiving and decrypting said first encrypted message to obtain said random key, means for encrypting transmissions to the decoder under said random key, said decoder having means to decrypt said transmissions received from the conditional access module.

11. Decoder according to claim 10, wherein said conditional access module comprises means for returning said

random key to the decoder in a second encrypted message with an authentication.

12. Decoder according to claim 11, wherein said generating means of the decoder further generates a random number which is included in said first encrypted message, wherein the conditional access module is adapted to use said random number as authentication in the second encrypted message.

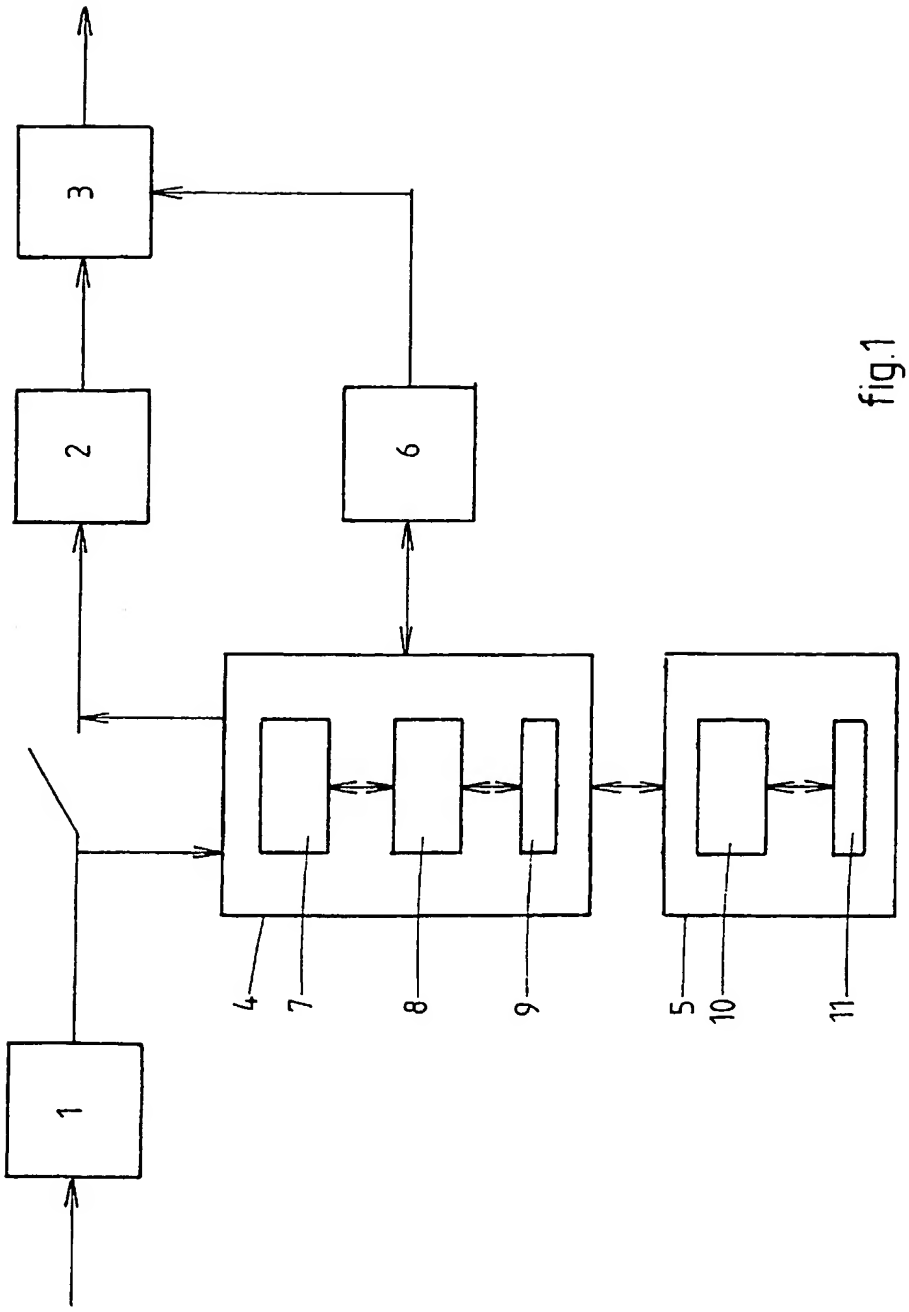


fig.1

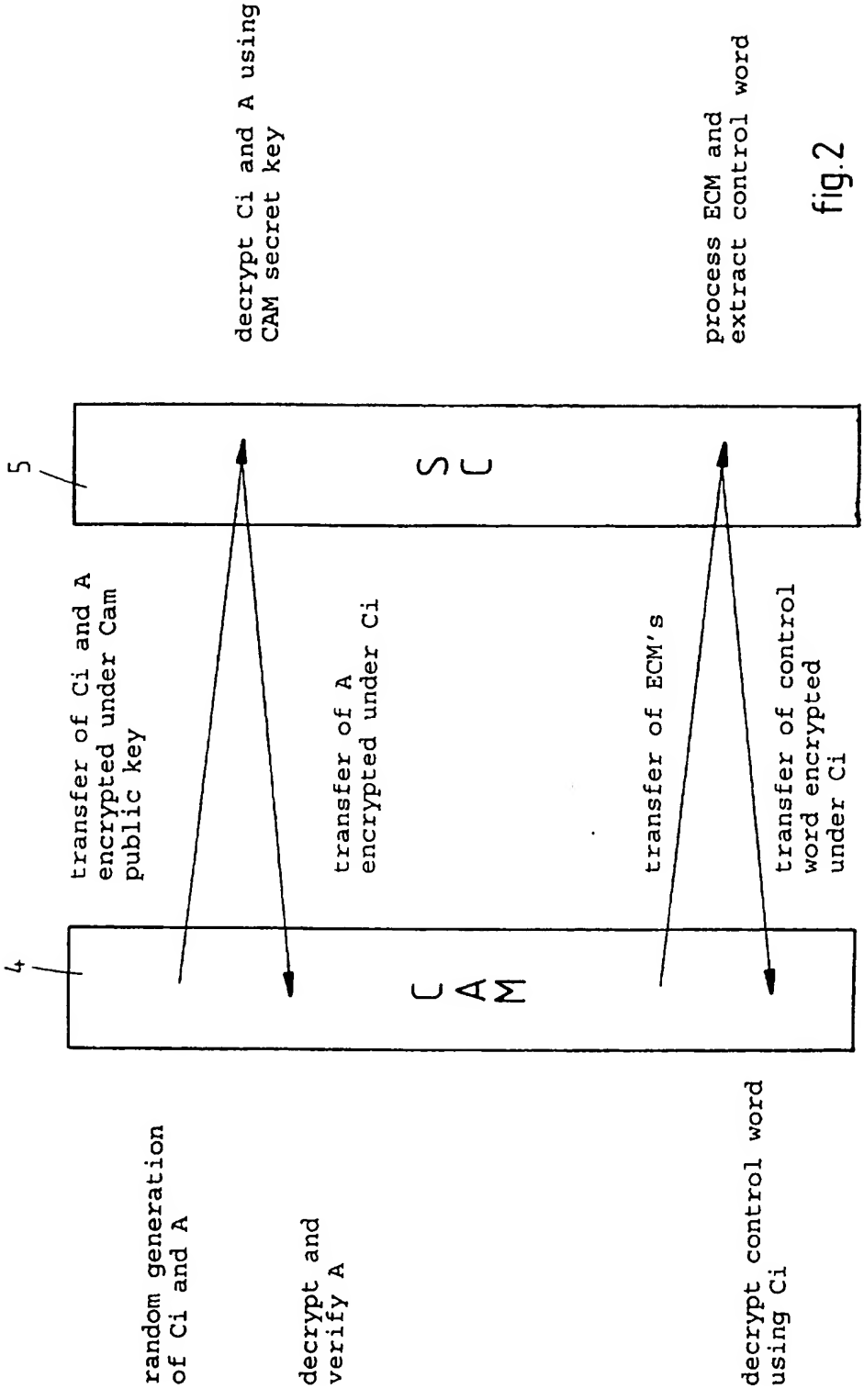

decrypt Ci and A using CAM secret key
process ECM and extract control word
5
S C
transfer of Ci and A encrypted under Cam public key
transfer of A encrypted under Ci
transfer of ECM's
transfer of control word encrypted under Ci
4
C A M
random generation of Ci and A
decrypt and verify A
decrypt control word using Ci

fig.2

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP 97/01557

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04N7/16 H04N7/167

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 658 054 A (NEWS DATACOM LTD) 14 June 1995 see column 1, line 37 - column 4, line 31 ---	1-12
A	IEEE TRANSACTIONS ON CONSUMER ELECTRONICS, vol. 35, no. 3, 1 August 1989, pages 464-468, XP000065971 COUTROT F ET AL: "A SINGLE CONDITIONAL ACCESS SYSTEM FOR SATELLITE-CABLE AND TERRESTRIAL TV" see the whole document ---	1-12
A	EP 0 428 252 A (NEWS DATA SECURITY PRODUCTS LT) 22 May 1991 see the whole document ---	1-12
	-/--	

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

1

Date of the actual completion of the international search	Date of mailing of the international search report
11 June 1997	- 4. 07. 97

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+ 31-70) 340-2040, Tx. 31 651 epo nl, Fax (+ 31-70) 340-3016	Greve, M

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP 97/01557

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 029 207 A (GAMMIE KEITH B) 2 July 1991 see abstract -----	1,7,10

1

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP 97/01557

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0658054 A	14-06-95	IL 107967 A	05-12-96
		AU 8034294 A	15-06-95
		CA 2137608 A	10-06-95
		JP 7288522 A	31-10-95
		US 5590200 A	31-12-96
EP 0428252 A	22-05-91	IL 92310 A	30-05-94
		AU 642157 B	14-10-93
		AU 6230690 A	23-05-91
		CA 2025585 A	15-05-91
		JP 3210843 A	13-09-91
		US 5481609 A	02-01-96
		US 5282249 A	25-01-94
US 5029207 A	02-07-91	AU 635180 B	11-03-93
		AU 7340291 A	21-08-91
		CA 2049310 A	02-08-91
		EP 0466916 A	22-01-92
		JP 4506736 T	19-11-92
		WO 9111884 A	08-08-91
		US 5237610 A	17-08-93